TrustBearer™ Desktop Software Guide

Version 0.1.1

Requirements

- Windows XP, Vista, or 2000 Service Pack 4 or higher
- PIV, CAC, Athena APCOS, JavaCard (with Muscle Applet)
- PC/SC compliant smart card reader
- TrustBearer Desktop Software

Overview

TrustBearer Desktop provides software for using smart cards for digital signing, authentication, and data protection for desktop based applications. TrustBearer Desktop requires that you have a digital id in order to begin using it for digital signing purposes. Once you have a digital id, you can begin using Outlook, and Adobe Acrobat for signing documents and mail.

Installation

Make sure you are logged in as a local Administrator user. Double click on the installer and follow the instructions for each screen.

Uninstallation

Make sure you are logged in as a local Administrator user.. Next in Control Panel, choose Add/Remove Programs. Click on TrustBearer Desktop and choose Remove. This will start the uninstaller. Once that has finished, reboot.

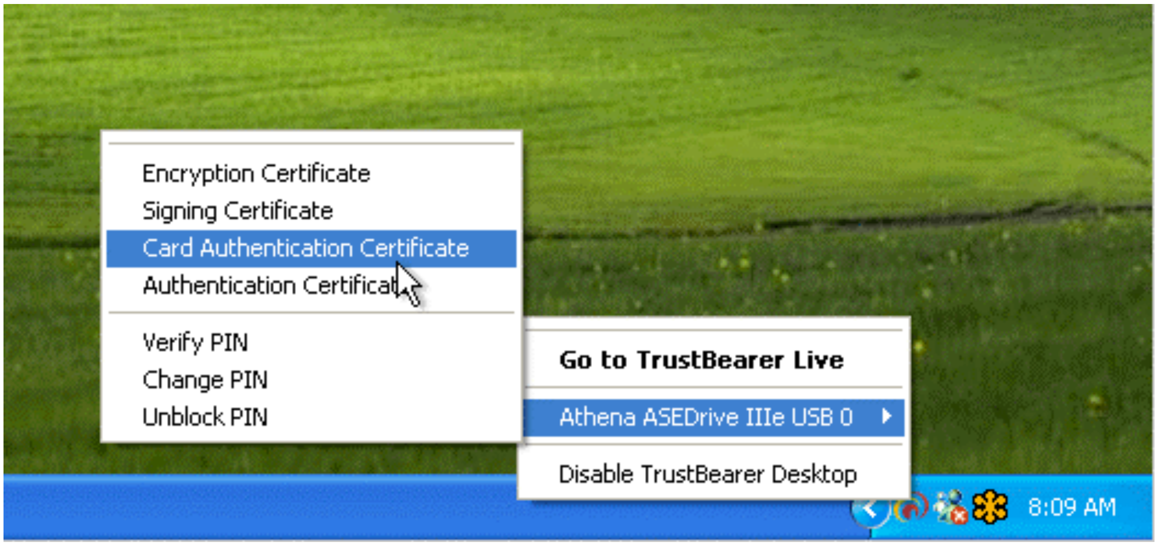
TrustBearer Desktop System Tray Overview

The system tray is where all TrustBearer Desktop capabilities can be accessed, which is capable of doing some of the following functions:

- Viewing and registering certificates
- Changing your user pin
- Modifying settings and preferences
- Unblocking your pin
- Visiting TrustBearer Live-enabled applications

TrustBearer Desktop is run when you login to your account. It sits in the system tray and has the TrustBearer logo like below:

By right clicking on this icon, menus and options will show up on screen.


Encryption Certificate
Signing Certificate
Card Authentication Certificate
Authentication Certificat
Verify PIN
Change PIN
Unblock PIN
Go to TrustBearer Live
Athena ASEDrive IIIe USB 0
Disable TrustBearer Desktop
8:09 AM

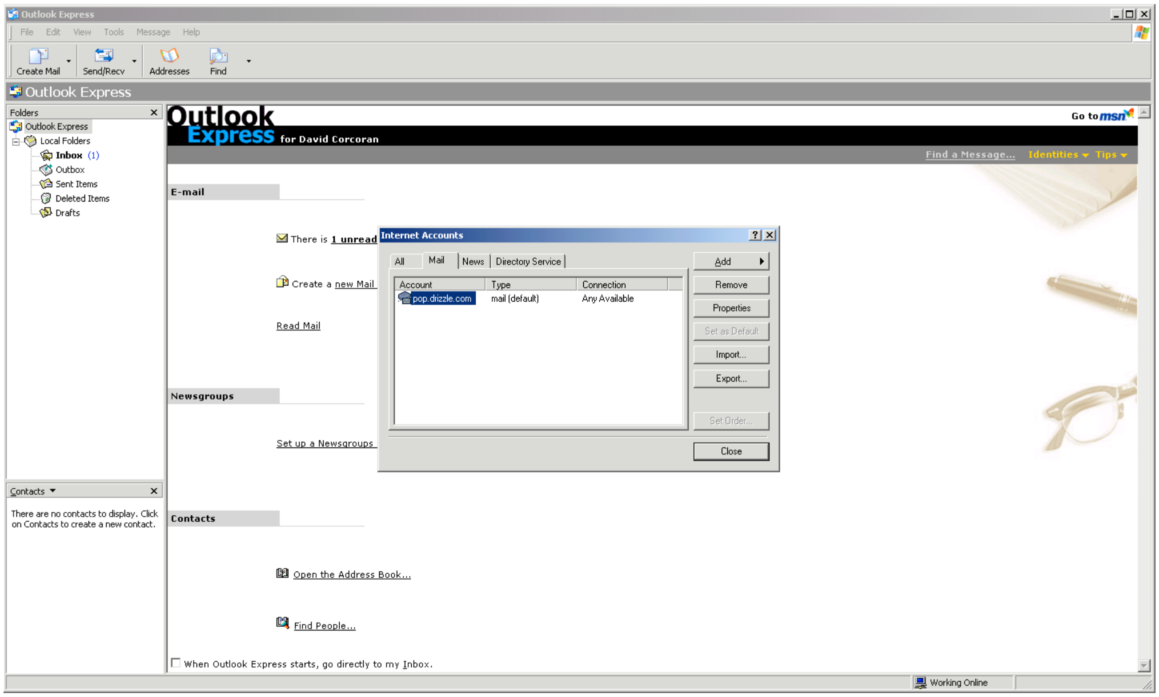
Some of these options will launch your default web browser to visit the appropriate online application. These options will take you to the appropriate trustbearer.com application server. Verify PIN and Change PIN are local to the machine.

In a commercial deployment scenario, the TrustBearer Live server would be deployed in house and TrustBearer Desktop would be configured to use that as its application server.

Secure Email using Outlook

Configuring Outlook Express

Once you have enrolled and trusted your digital id you can configure Outlook to use your smart card for signing and decryption of emails. In order to use Outlook for this purpose you must have previously enrolled for a certificate on your smart card and installed it on your computer. This was described in another section of the User Manual. To begin, open Outlook Express



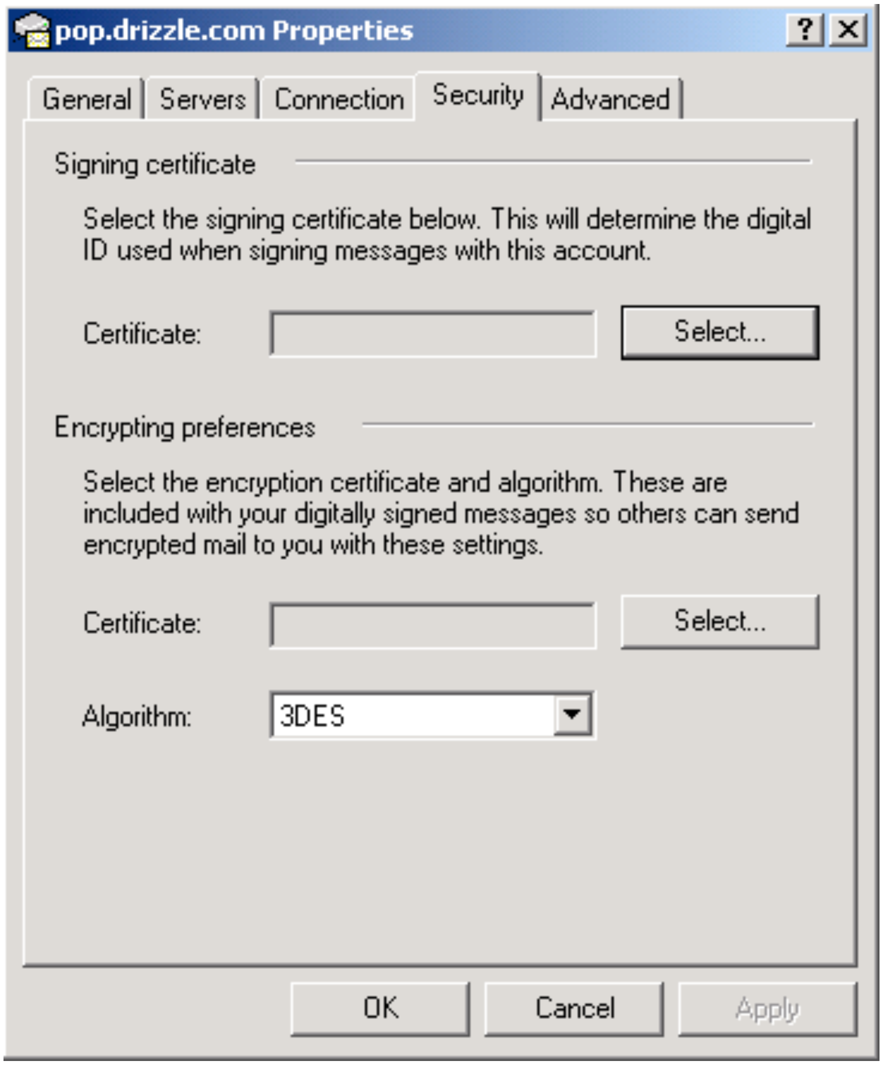
Account	Type	Connection
pop.drizzle.com	mail (default)	Any Available

In the menu, choose: <u>Tools -> Accounts</u>. Choose the Mail pane and you will see a similar dialog to the one above. Select the email account you wish to use your smart card with.

The email address your account is configured with must be the same as the one here.

Once you have selected the correct account, choose: <u>Properties</u>.

Select the Security pane from the available panes. You should see a dialog such as the following.



Signing certificate

Select the signing certificate below. This will determine the digital ID used when signing messages with this account.

Certificate:

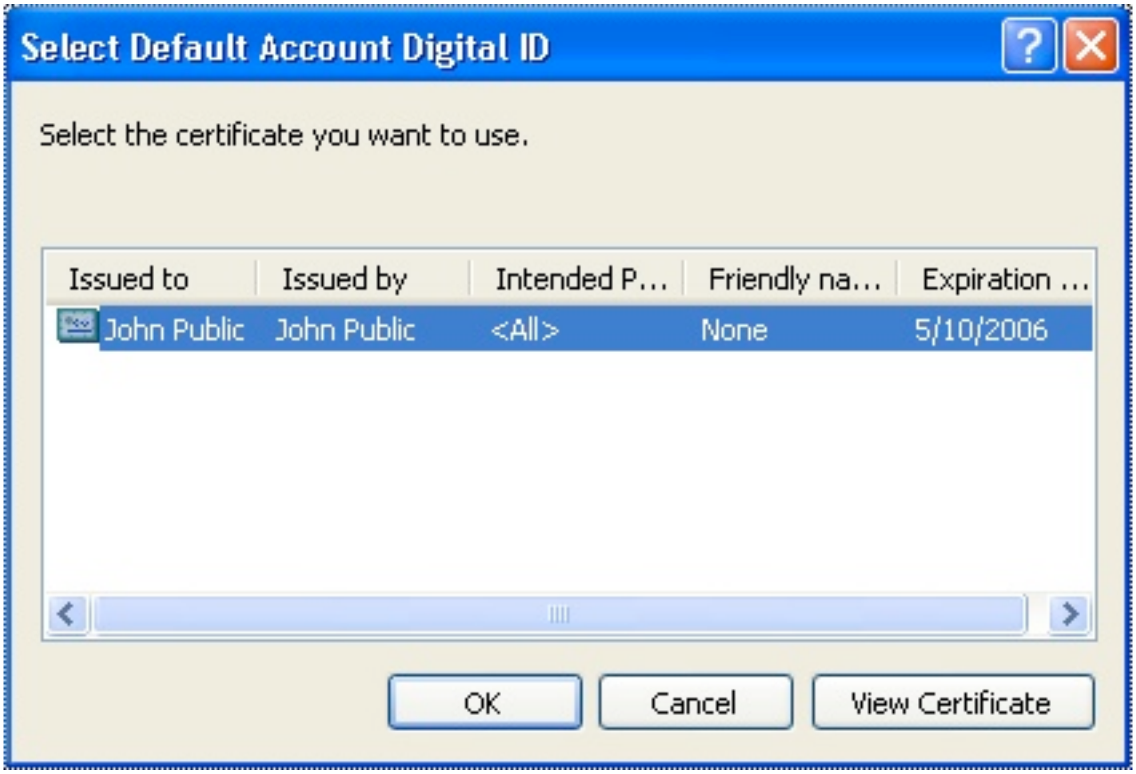
Encrypting preferences

Select the encryption certificate and algorithm. These are included with your digitally signed messages so others can send encrypted mail to you with these settings.

Certificate:

Algorithm: 3DES

Now, we will select the certificate we wish to use for this email account. Choose the top: Select button and you will be presented with the certificate selection dialog (next page)



Select Default Account Digital ID

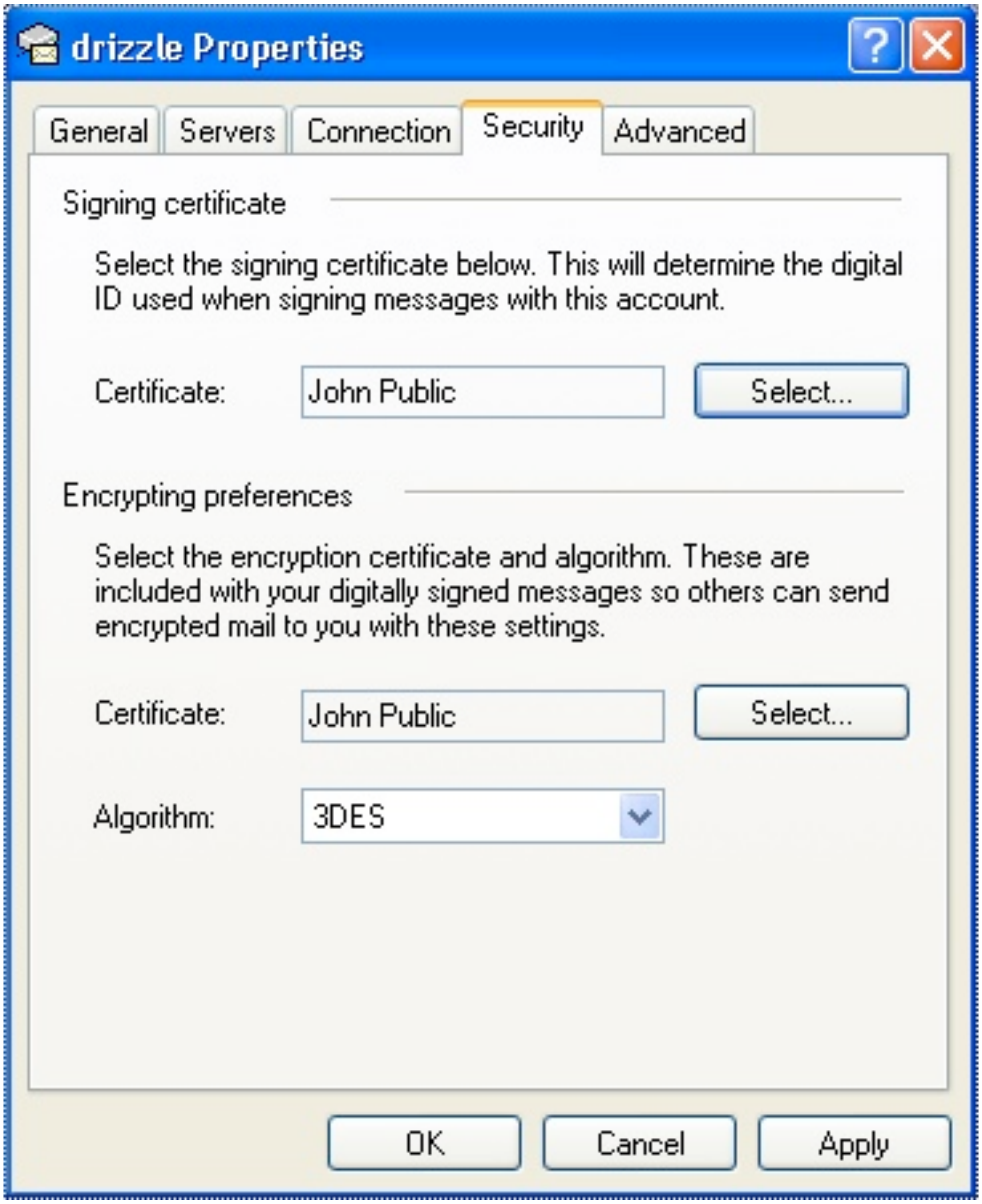
Select the certificate you want to use.

Issued to	Issued by	Intended P...	Friendly na...	Expiration ...
John Public	John Public	<All>	None	5/10/2006

Choose the certificate you enrolled your smart card with from the list of available certificates. Choose: OK

Once you have chosen the certificate to be used as your signing certificate, now choose the bottom Select button to select the encryption certificate. You will be presented with a dialog similar to the one above. Choose the certificate you wish to use for encryption.

You should now have a Security pane, which contains the certificates you have chosen for Signing and Encryption. It should look similar to the following:



drizzle Properties

Signing certificate

Select the signing certificate below. This will determine the digital ID used when signing messages with this account.

Certificate: John Public

Encrypting preferences

Select the encryption certificate and algorithm. These are included with your digitally signed messages so others can send encrypted mail to you with these settings.

Certificate: John Public

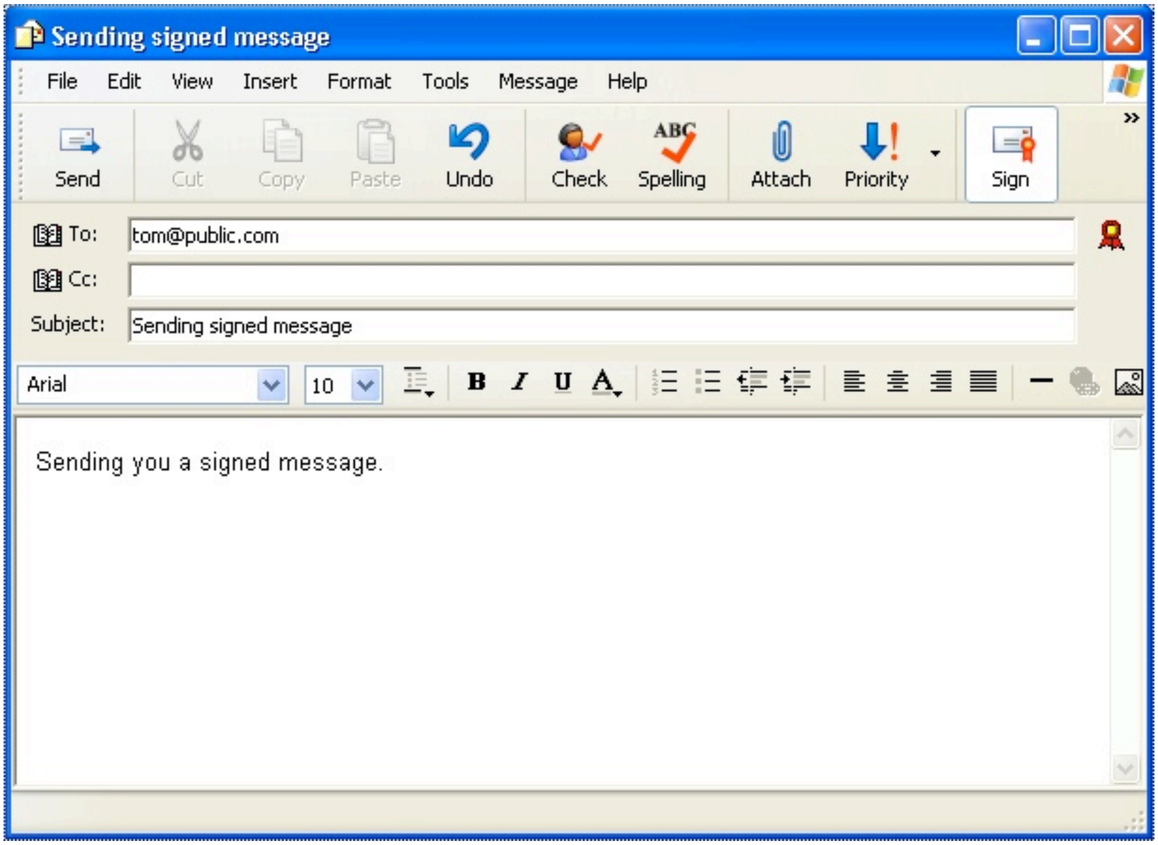
Algorithm: 3DES

The name of your certificate may vary from that shown in the above dialog.

Sending Secure Mail

Compose an email and choose Sign from the button bar above to digitally sign your mail Choose Encrypt to encrypt the mail.

You must have the encryption certificate of the person whom you wish to send an encrypted mail to if you choose to encrypt the mail.



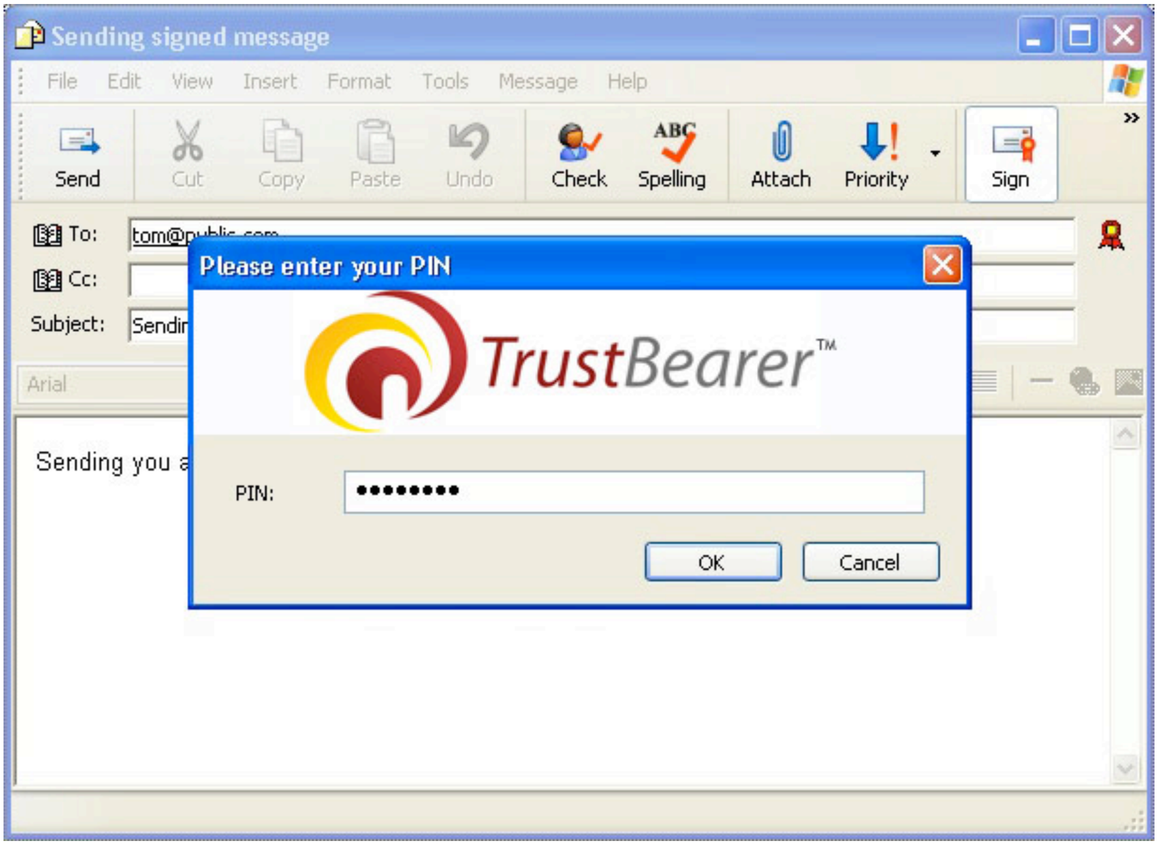
To: tom@public.com

Cc:

Subject: Sending signed message

Sending you a signed message.

You will be asked for your smart card's Personal Identification Number (PIN)



To: tom@public.com

Cc:

Subject: Sendir

Sending you a

Please enter your PIN

PIN: •••••••••

Enter your PIN and choose: OK

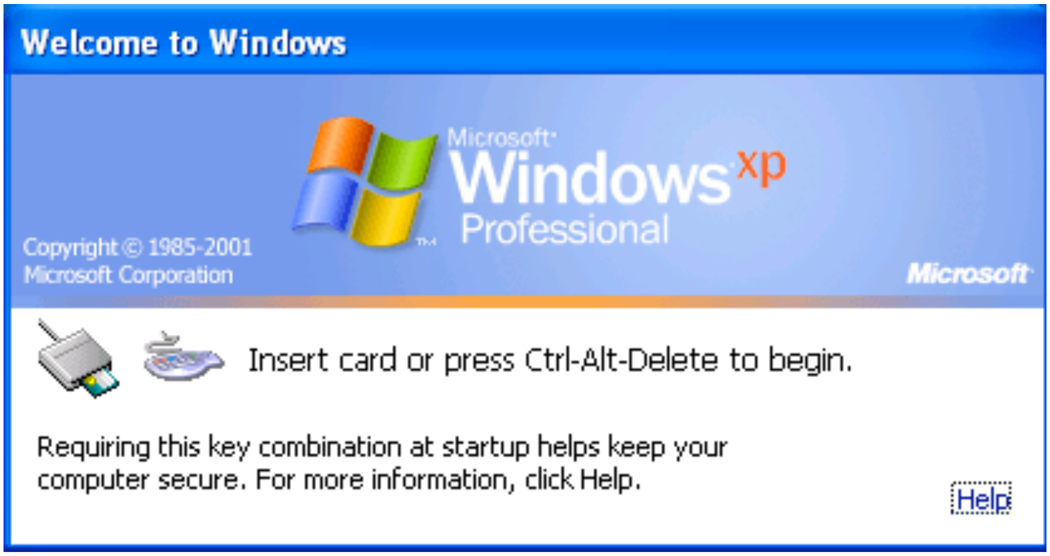
Notes:

There may be a short delay as the system assesses the smart card to sign the message.

You will be prompted for your PIN if someone has sent you an encrypted email which was encrypted using the certificate stored on your smart card.

Smart Card Login

Upon enrollment for a certificate, your smart card can be immediately used for smart card login. Make sure your smart card reader is plugged in and operating correctly. Logout of your account or restart the computer until the Windows login screen appears. It should appear as below.



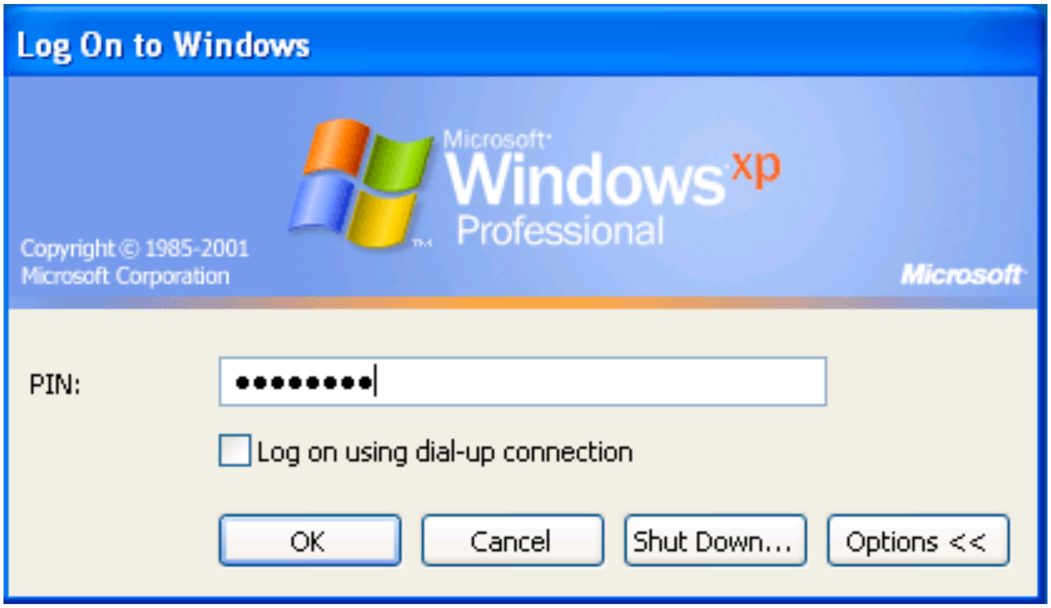
Welcome to Windows

Insert card or press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

It is important that it states, "Insert card or press Ctrl-Alt-Delete". If it does not show this screen, make sure your reader is working properly. Also refer to the FAQ's or Administrative Guide for help.

Remove and insert or insert your smart card into your smart card reader. The previous dialog will request for your Personal Identification Number (PIN).


Log On to Windows
Microsoft Windows xp Professional
Copyright © 1985-2001 Microsoft Corporation
Microsoft
OK
Cancel
Shut Down...
Options <<

PIN: •••••••••

□ Log on using dial-up connection

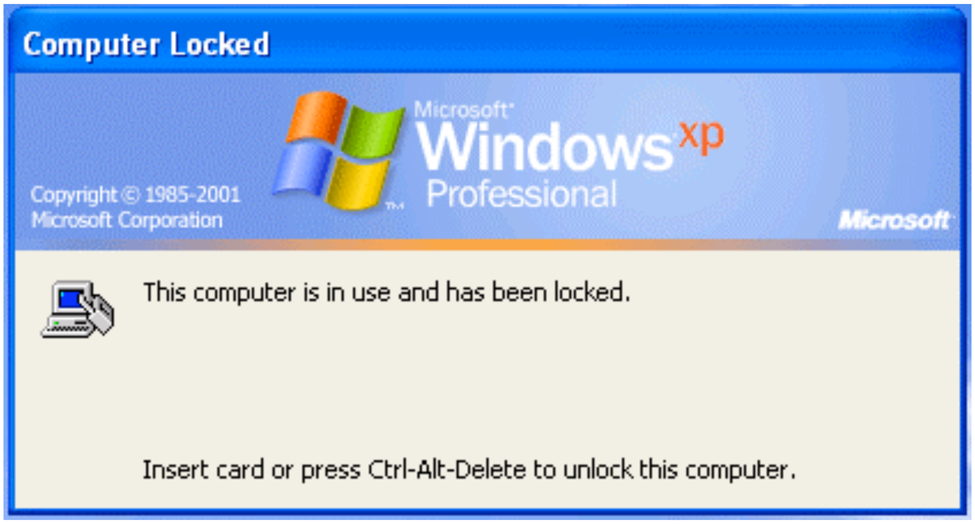
Enter your PIN and choose: OK

Windows will now proceed to log you in using your smart card.

Do not remove the smart card during the login process.

Screen Lock

Windows can be configured to lock the workstation when the smart card is removed from the reader. This can be configured through the registry. Please refer to the FAQ for more information on configuring screen lock. When configured, removal of the smart card will result in the following screen.

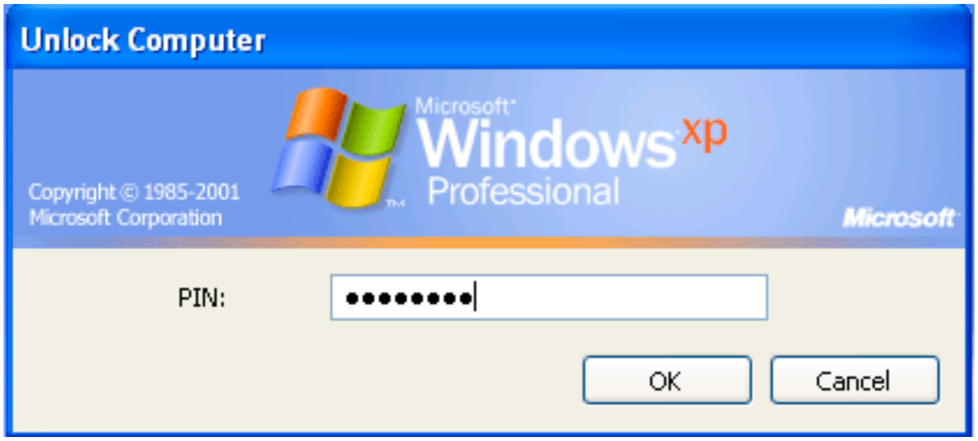


Computer Locked

This computer is in use and has been locked.

Insert card or press Ctrl-Alt-Delete to unlock this computer.

Insertion of the card will present you with the PIN dialog. Enter your PIN and choose: OK to log back into the machine.

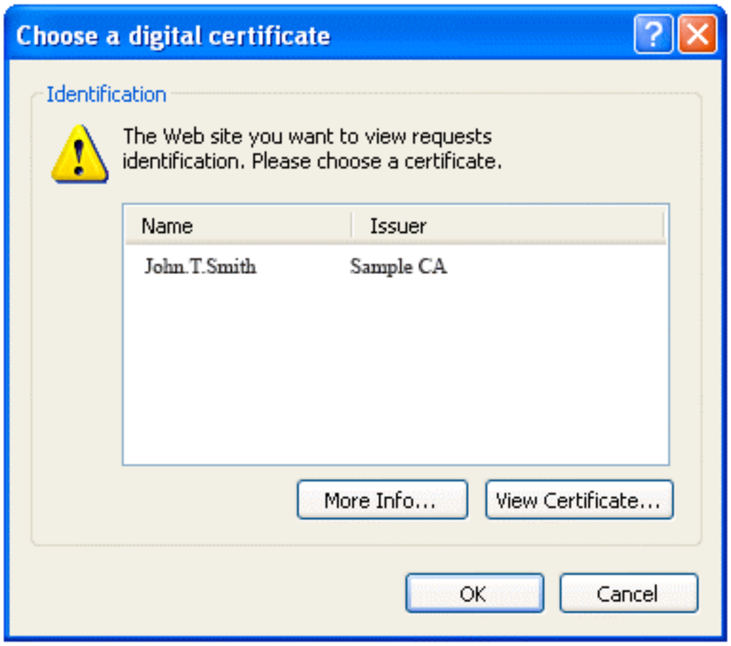


Unlock Computer

PIN: ●●●●●●●●●

Web Authentication

Some web sites can be configured to require SSL authentication and possibly a smart card to access them. Internet Explorer will make use of your certificates and card when needed for authentication. Internet Explorer will first ask you to choose the certificate you wish to authentication with.



Choose a digital certificate

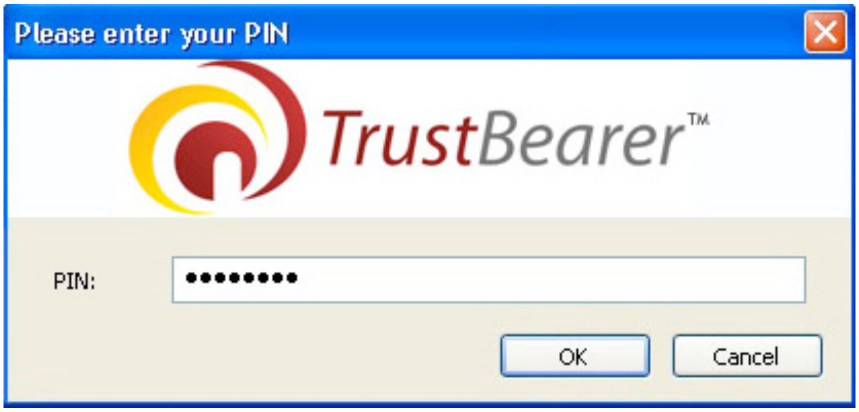
Identification

The Web site you want to view requests identification. Please choose a certificate.

Name	Issuer
John.T.Smith	Sample CA

Once you have selected the certificate you wish to use, choose: OK

Next you may be presented with the PIN dialog. Enter your PIN and choose: OK



Please enter your PIN

PIN: •••••••••

If the website appears, you have successfully authenticated using your card.

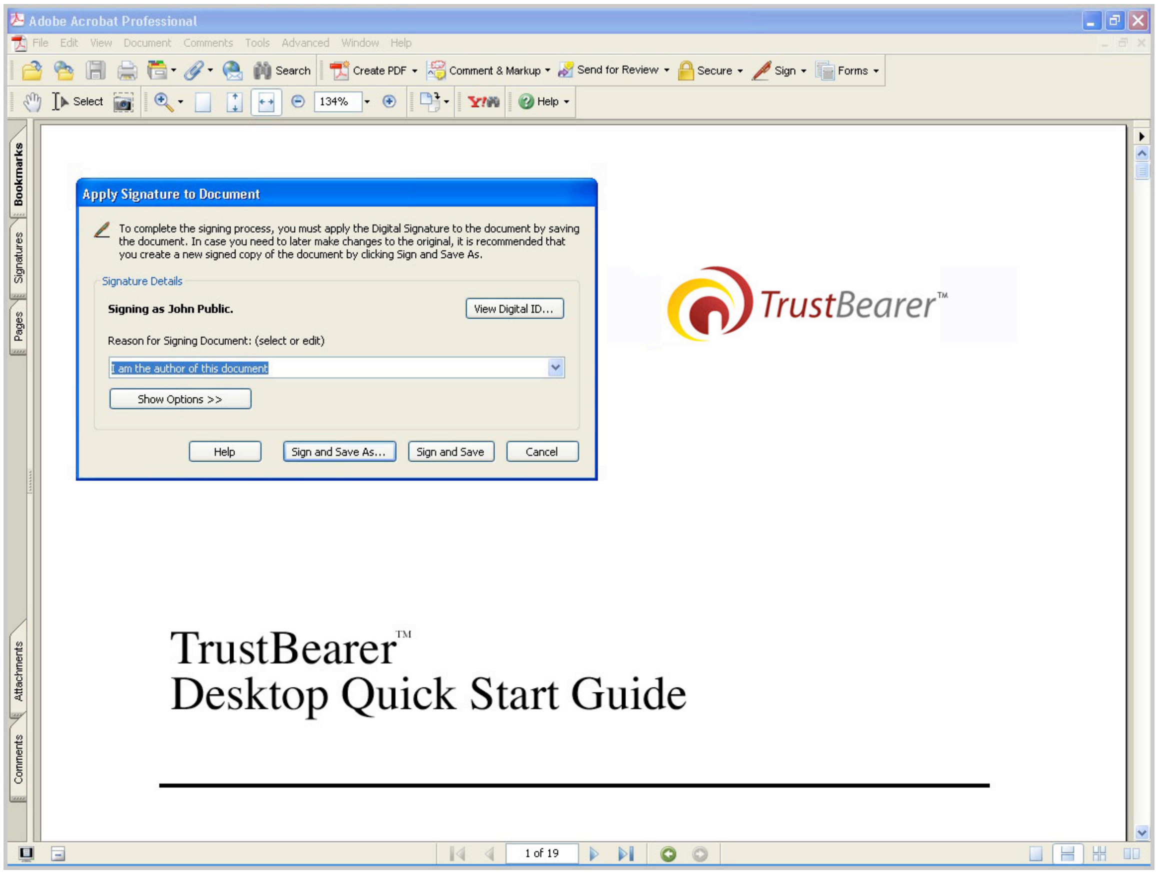
Signing Documents with Adobe Acrobat

Once you have enrolled and trusted your digital id, you can use it to sign documents with Adobe Acrobat.   Open a PDF document and choose in the menu:

Document->Digital Signatures->Sign this Document

Choose whether you wish to create a new signature field to sign or whether the signature field is invisible. Creating a signature field to sign shows the signature on the document. We will choose this option.

Use the mouse to drag an area where you wish the signature to be placed. Once done, the pin dialog will prompt you for your user pin. It will then ask you the reason for signing the document and if you have multiple digital id's, will give you the option of choosing one. It should look like below:



Apply Signature to Document

To complete the signing process, you must apply the Digital Signature to the document by saving the document. In case you need to later make changes to the original, it is recommended that you create a new signed copy of the document by clicking Sign and Save As.

Signature Details

Signing as John Public.

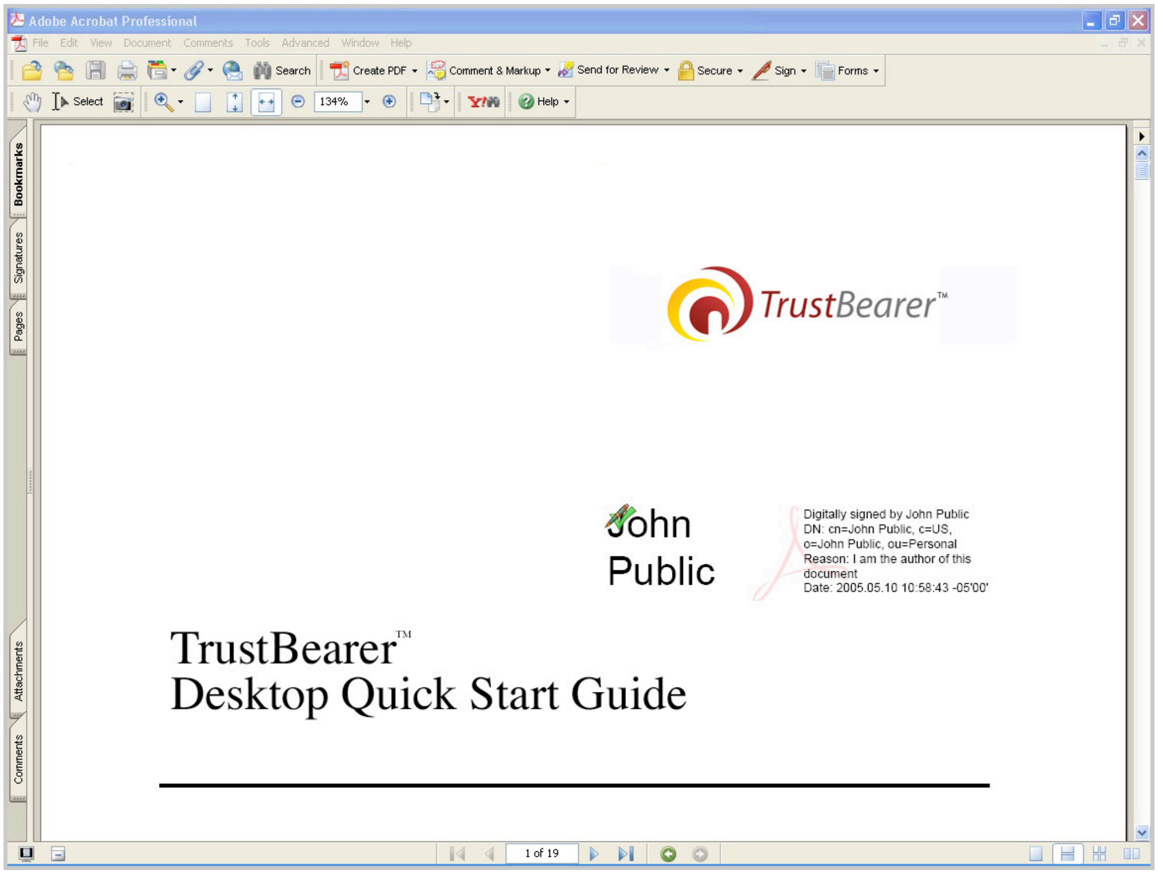
Reason for Signing Document: (select or edit)

I am the author of this document

TrustBearer™
Desktop Quick Start Guide

Choose your reason for signing (example: I am the author of this document) and then Sign and Save. In a few moments it will sign and save the document. You should see the valid signature as displayed:

Signed document with Adobe:



John Public

Digitally signed by John Public
DN: cn=John Public, c=US,
o=John Public, ou=Personal
Reason: I am the author of this
document
Date: 2005.05.10 10:58:43 -05'00'

TrustBearer™
Desktop Quick Start Guide

The document now contains a digital signature showing ownership of the document. Several people can sign these documents and sign areas of them as they develop them. TrustBearer Desktop can be used for multiple people to sign documents as they are passed around for authorship and review.

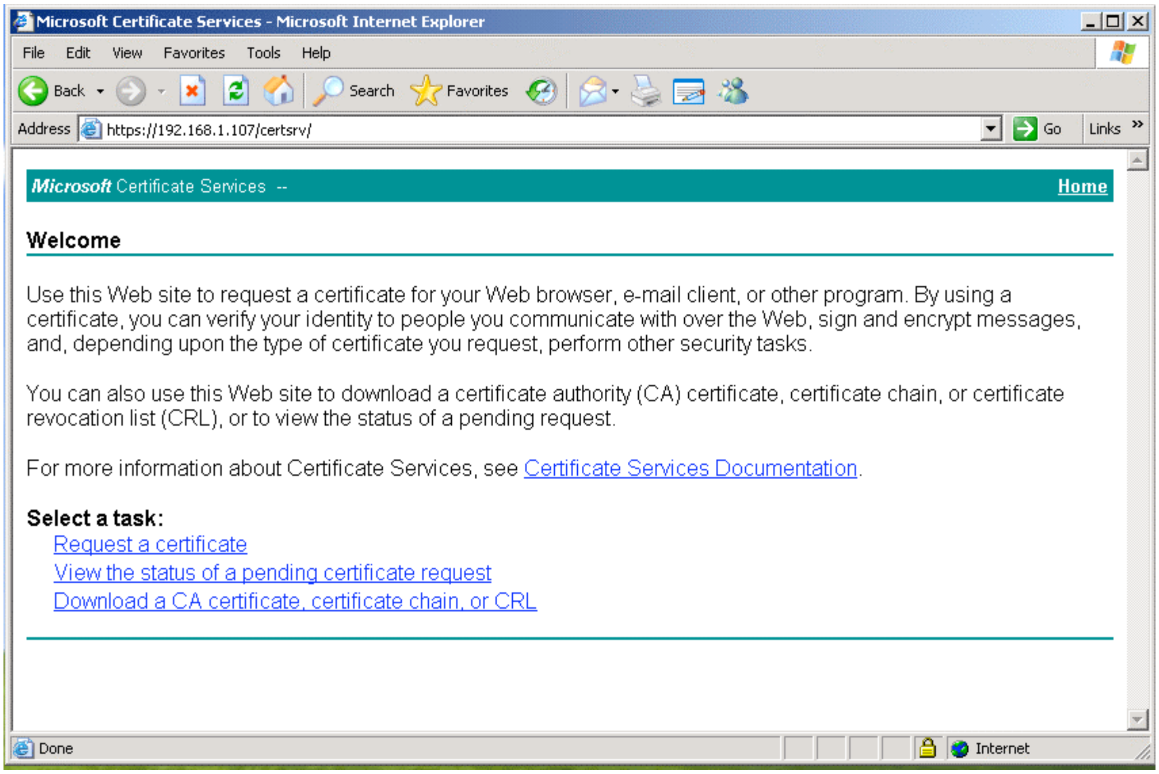
Certificate Enrollment

A user must enroll for a certificate prior to using the services, which Microsoft provides for smart cards. Windows 2003 must be configured to issue certificates to smart cards. Please refer to the Administrative Guide for information on configuring your Windows 2003 server. It must be configured before proceeding.

Windows 2003 provides a certificate enrollment station to users, which belong to the domain. To reach the enrollment website, open Internet Explorer and go to:

https://myservername/certsrv

You may be asked to trust the website you are attempting to connect to. Allow your web browser to connect. Once a connection has been established you will be presented with a dialog-requesting authentication. Enter the username and password of the account, which you wish to issue a smart card certificate to. Once you have successfully authenticated you will be presented with the following site:


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Done
Internet

https://192.168.1.107/certsrv/

Microsoft Certificate Services -- Home

Welcome

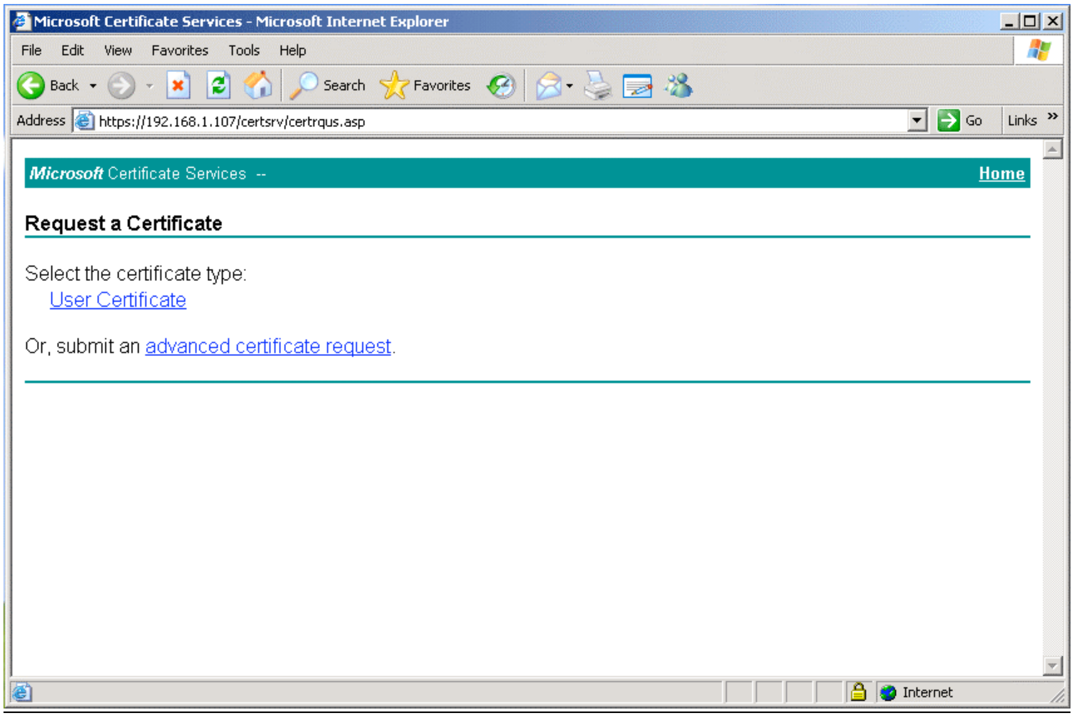
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

From the certificate enrollment page choose: Request a certificate.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.1.107/certsrv/certrqus.asp
Go Links
Internet

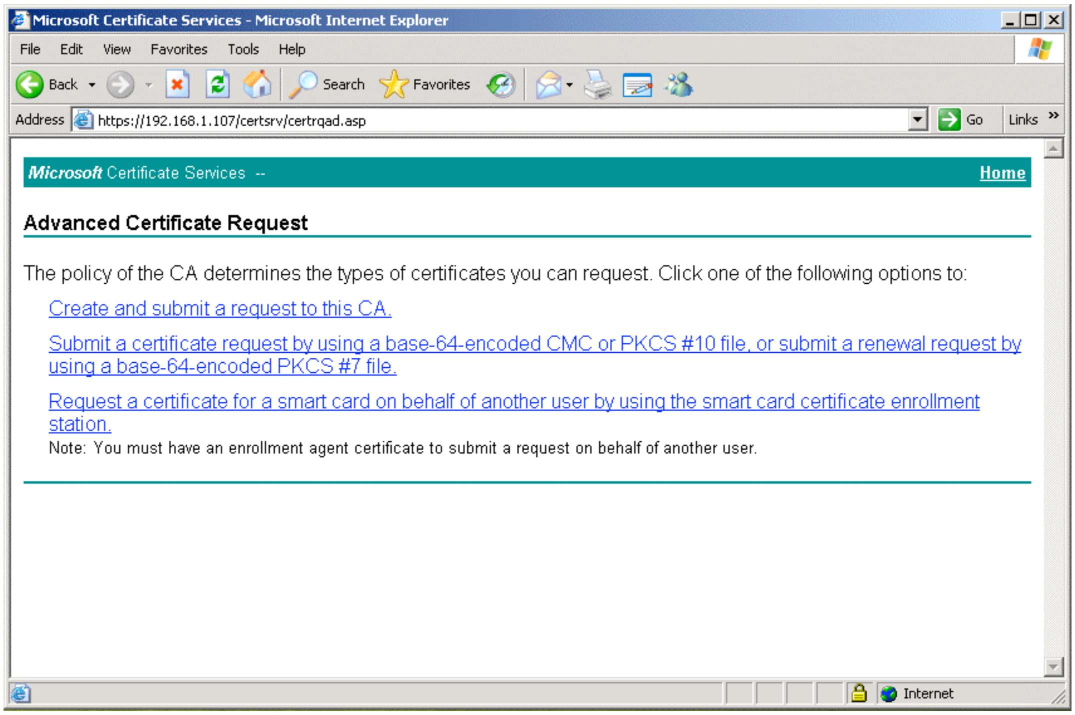
Microsoft Certificate Services -- **Home**

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Choose: advanced certificate request



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.1.107/certsrv/certrqad.asp
Go Links
Internet

Microsoft Certificate Services -- **Home**

Advanced Certificate Request

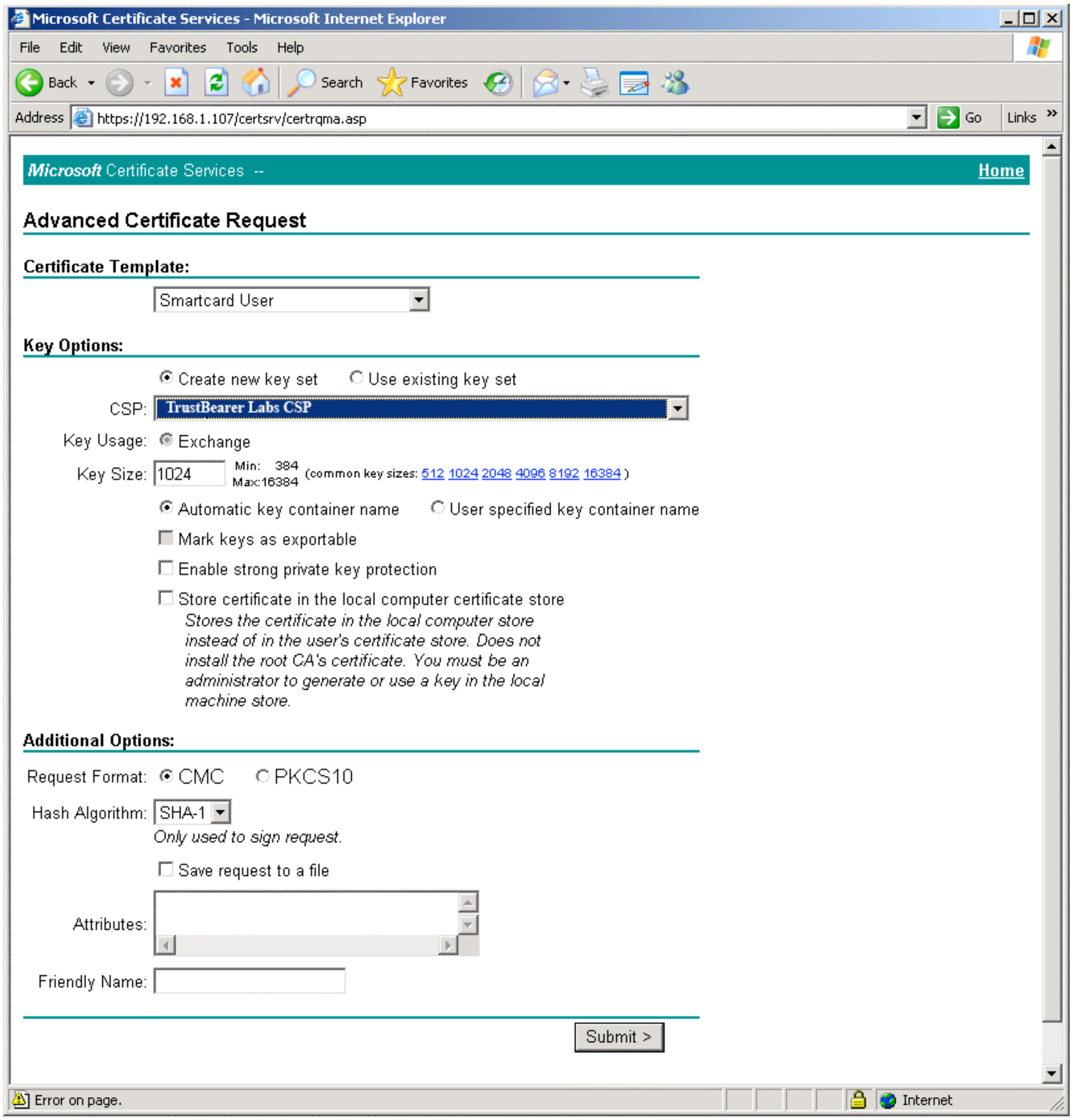
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Choose: Create and submit a request to this CA


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Home
Submit >
Error on page.
Internet

https://192.168.1.107/certsrv/certrqma.asp

Microsoft Certificate Services --

Advanced Certificate Request

Certificate Template:

Smartcard User

Key Options:

● Create new key set ○ Use existing key set

CSP: TrustBearer Labs CSP

Key Usage: ● Exchange

Key Size: 1024 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

□ Mark keys as exportable

□ Enable strong private key protection

□ Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: ● CMC ○ PKCS10

Hash Algorithm: SHA-1

Only used to sign request.

□ Save request to a file

Attributes:

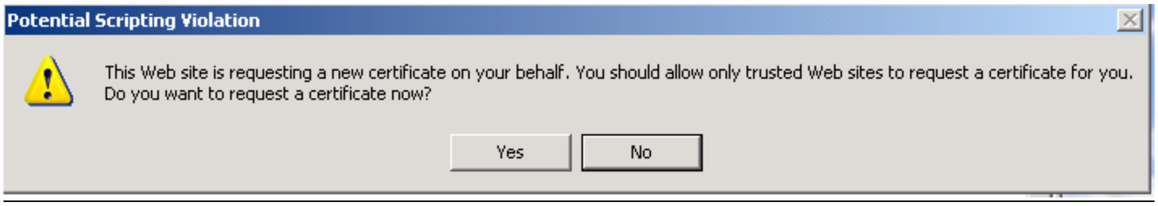
Friendly Name:

You will be presented with the Advanced Certificate Request page. From this page be sure that you select Smartcard User as the certificate template from the list of template options. If you do not see an option for Smartcard User, please refer to the Administrative Guide to learn how to configure this option.

Be sure a supported and pre-personalized smart card resides in your smart card reader and that the reader is fully functional and powered up.

From the list of available CSP's, choose TrustBearer Labs CSP from the list. All other options should remain defaults and should be exactly how they look in the above figure.

Choose : Submit

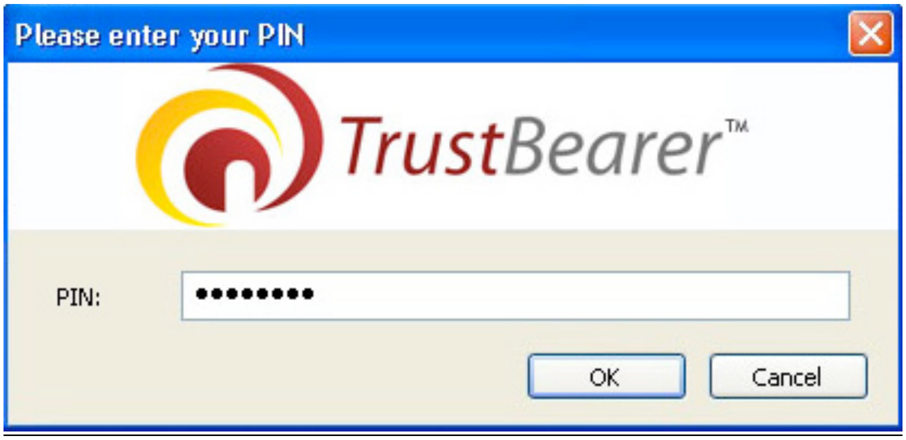


This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?

You will be asked if you are sure you want to request a certificate on your behalf

Choose: Yes

There may be a short delay as your smart card is being accessed.

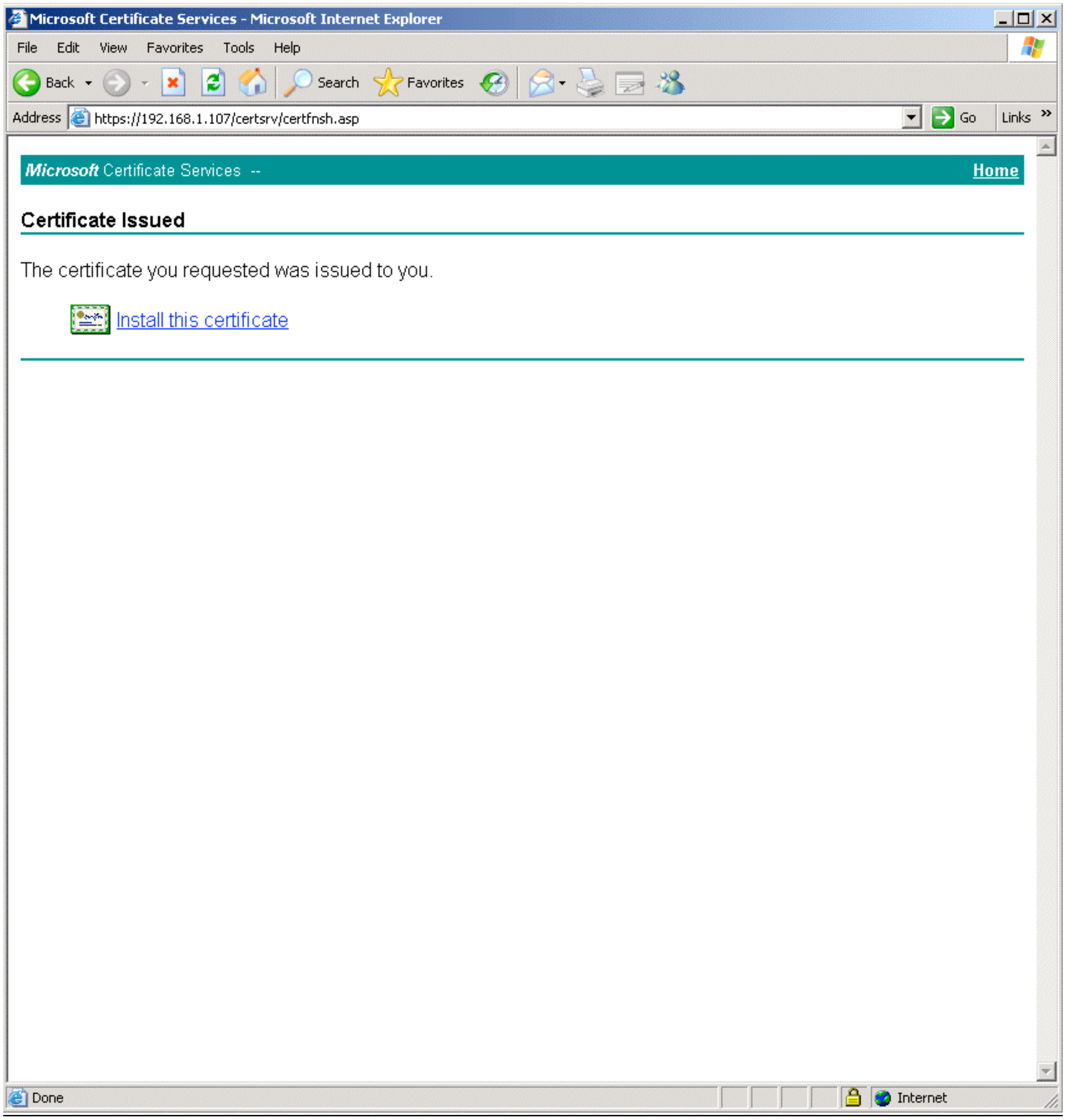


PIN: •••••••••

You will be asked to enter your Personal Identification Number (PIN), which you set during pre-personalization. Enter that pin in the text dialog.

Enter your PIN and choose: OK

There may be a short delay as your smart card is being accessed.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.1.107/certsrv/certfnsh.asp
Go Links
Microsoft Certificate Services --
Home
Done
Internet

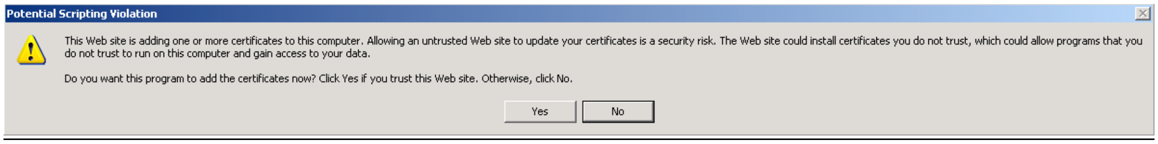
Certificate Issued

The certificate you requested was issued to you.

Install this certificate

The certificate enrollment has issued a certificate to your smart card. You must now install this certificate onto your computer.

Choose: Install this certificate



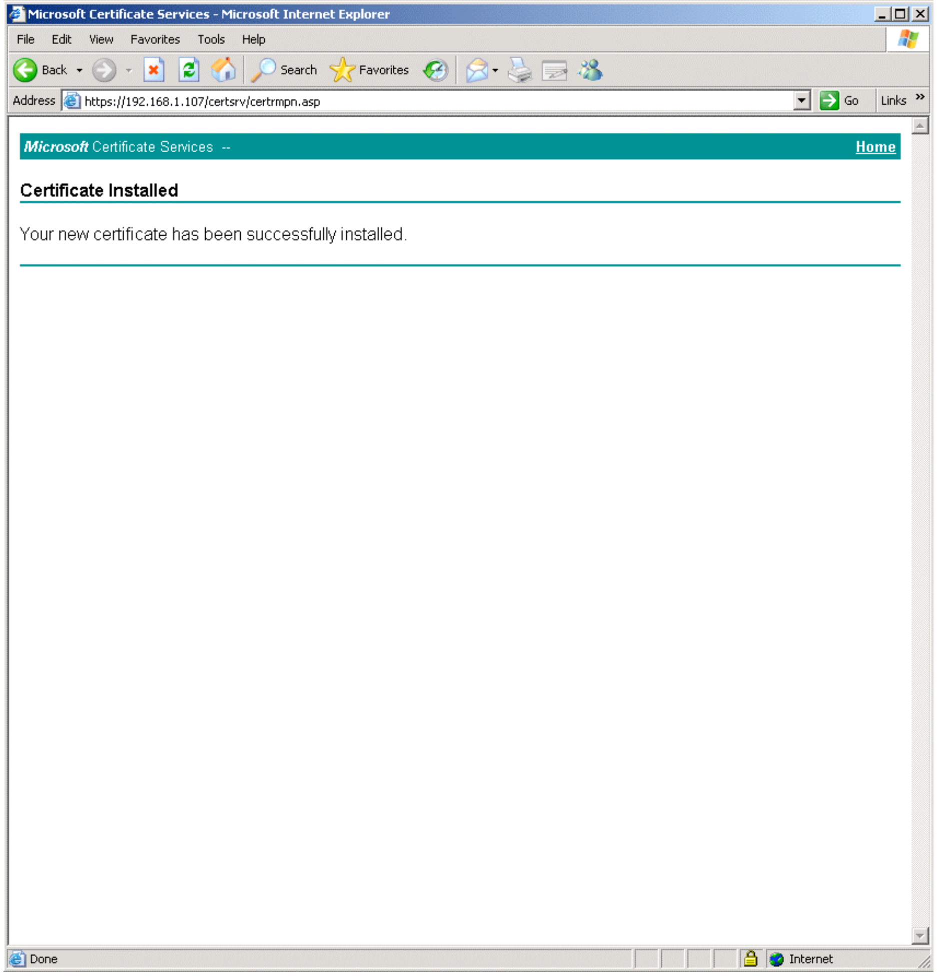
This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

You will be asked whether you really want to install this certificate.

Choose: Yes

There may be a short delay as your smart card is being accessed.



Microsoft Certificate Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
Go
Links
Microsoft Certificate Services --
Home
Done
Internet

https://192.168.1.107/certsrv/certrmpn.asp

Certificate Installed

Your new certificate has been successfully installed.

Your certificate has now been installed. Please refer to the other portions of the manual to learn how to use your fully personalized card. (You may close Internet Explorer)

Technical Addendum

Architecture

This product provides the following software components:

Microsoft Cryptographic Service Provider (CSP)

The CSP provided allows the smart card to be plugged into the Microsoft CryptoAPI infrastructure allowing applications, which use CryptoAPI to make use of the smart card.

PKCS#11 Module

The PKCS#11 module provided allows applications, which use PKCS#11 to use of the smart card.

Dynamic Service Modules (DSMs)

This layer contains the platform independent DSM's which abstract specific device implementations and data models. There is both an installed DSM directory and a per-user cache of DSM's.

System Tray Application

The system tray application is configurable and provides basic functionality and the ability to link off to TrustBearer Live enabled applications through the web browser.

File Structure

The product installs the following relevant files onto the host computer:

INSTALL DIRECTORY (Example: C:\Program Files\TrustBearer Labs)

- TBCSP.dll (CSP Component)
- TBLIVE.dll (PKCS#11 Component)
- DSM (Specific DSM’s & Cache Links)

Registry Settings

This software adds or modifies the following registry components:

CSP

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\
Calais\SmartCards\TBDesktopCard_xxxxxxxx

ATR	BINARY	<ATR VALUE>
ATRMask	BINARY	<ATR MASK VALUE>
Crypto Provider	STRING	TrustBearer Labs CSP

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\
Defaults\Provider\TrustBearer Labs CSP

Image Path	STRING	<PATH TO CSP>
PKCS11Module	STRING	<PATH TO PKCS#11 MODULE>
SigInFile	DWORD	0
Type	DWORD	1
Logging	DWORD	1 – turn logging on, 0 – turn logging off
LogFileName	STRING	<PATH TO LOGFILE, default: C:\CSPDEBUG.log>

TrustBearer Desktop/Live

HKEY_LOCAL_MACHINE\SOFTWARE\TrustBearer Labs\TBLive
HKEY_LOCAL_USER\SOFTWARE\TrustBearer Labs\TBLive

AllowTrayRegLogon	DWORD	1 – yes, 0 – no
DSMCacheDir	STRING	<PATH TO DSM DIRECTORY>
Logging	DWORD	1 – turn logging on, 0 – turn logging off
LogFileName	STRING	<PATH TO LOGFILE, default: C:\tblive.log>

Frequently Asked Questions (FAQ)

Q: My card does not seem to trigger the Windows login PIN dialog
A: Make sure you have a working reader plugged in and that your card has been introduced to the system. For more information on this, see Introducing Card Types.

Q: How can I get detailed logging information?
A: You can turn on logging in several locations. See the section on registry settings for more information. Higher-level Windows logs can be viewed in the event viewer.

Q: Logging shows that my token is unrecognized
A: Make sure your card or device is supported by TrustBearer Desktop.

Q: Where is a PKCS#11 module I can load into my application?
A: It is contained in PROGRAM_FILES\TrustBearer Labs\TBLive.dll.

Q: Windows login does not seem to work
A: Make sure your machine has been joined to the domain and that your client machine points it's DNS to the domain controller. If the PIN dialog never comes up, make sure your card reader is working and that your card is recognized by the system. You may need to register your card for login. Edit the AllowTrayRegLogon registry setting and in the system tray click "Register Card for Login" and reboot.

Q: The Smart Card User certificate template does not show up in the available templates.
A: Make sure you have granted Authenticated Users the ability to Read and Enroll that template. Also make sure you have set your CA the ability to issue it.

Q: The screen does not seem to lock when I remove my card
A: Make sure the ScRemoveOption is set in the registry.

Q: My browser will not connect to the certificate enrollment station
A: Your browser may have security settings not allowing Active X and other code to run in your browser. Check your browser's security settings. Also, make sure IIS is not configured to require client side certificate authentication. You cannot authenticate with a certificate that you have not enrolled for yet.